AMENDMENTS TO THE CLAIMS

1. **(CURRENTLY AMENDED)** A credential communication device adapted to transmit and receive data, including:

   a. means to process said data in order to effect mutual credential verification and ~~trusted~~ mutual recognition between the device and a second credential communication device, without reference to a third party, ~~further including~~

   b. at least one proximity conductor adapted to be controlled to transmit and receive at least some data ~~only when in such physical proximity to a second credential communication device as to effectively exclude the possibility of third party involvement in the transmission and reception of said data,~~

   c. means to effect variation in the power output of the proximity conductor in relation to the data to be transmitted, wherein in use:

      (1) selected data, which is data whose unauthorized reception is acceptable, is transmitted by the proximity conductor at such power as to be received by the second credential communication device before the credential exchange device establishes a physical proximity to the second credential communication device that effectively excludes the possibility of third party involvement in the transmission and reception of data, and

      (2) other selected data, which is data whose unauthorized reception is not acceptable, is transmitted by the proximity conductor at such a power as to be received by the second credential communication device only when the credential exchange device is in such physical proximity to the second credential exchange device that the possibility of third party involvement in the transmission and reception of data is effectively excluded.

2. **(CURRENTLY AMENDED)** A credential communication device as in claim 1, further adapted to require a user of the device to authenticate ~~**their**~~ **the user's** identity to the credential communication device immediately before communication with the second credential communication device.

3. **(PREVIOUSLY PRESENTED)** A credential communication device as in claim 1 further adapted to accept identity authentication by the keying of a pass code into the device.

4. **(PREVIOUSLY PRESENTED)** A credential communication device as in claim 1 further adapted to accept identity authentication by use of a biometric authentication apparatus.

5. **(PREVIOUSLY PRESENTED)** A credential communication device as in claim 1 wherein the proximity connector is an induction connection.

6. **(CURRENTLY AMENDED)** A credential communication device as in claim 5, wherein the induction connection is effected by a RF transceiver of such power as to require the physical proximity to ~~**be such as approximates**~~ **approximate** physical touch.

7. **(CANCELED)**

8. **(CURRENTLY AMENDED)** ~~**A credential communication device as in claim 1**~~ **A credential communication device adapted to transmit and receive data, including:**

   a. means to process said data in order to effect mutual credential verification and mutual recognition between the device and a second credential communication device, without reference to a third party,

   b. at least one proximity conductor adapted to be controlled to transmit and receive at least some data only when in such physical proximity to a second credential communication device as to effectively exclude the possibility of third party involvement in the transmission and reception of said data,

   wherein the proximity conductor includes a detector adapted to detect that physical touch is being maintained between the device and a second device, the device further adapted to transfer some data only when such touch is detected.

9. **(PREVIOUSLY PRESENTED)** A credential communication device as in claim 8 wherein the detector adapted to detect physical touch is a pressure sensor.

10. **(CURRENTLY AMENDED)** A credential communication device as in claim 1 wherein the proximity ~~**connector**~~ **conductor** is protected from physical or environmental damage by a thin layer or shell of material.

11. **(PREVIOUSLY PRESENTED)** A credential communication device as in claim 1 including means to communicate the results of processing to effect credential verification.

12. **(CURRENTLY AMENDED)** A credential communication device as in claim 11 wherein said communication means includes at least one ~~**trusted**~~ light indicator.

13. **(CURRENTLY AMENDED)** ~~**A credential communication device as in claim 11**~~ **A credential communication device adapted to transmit and receive data, including:**

a. means to process said data in order to effect mutual credential verification and mutual recognition between the device and a second credential communication device, without reference to a third party,

b. at least one proximity conductor adapted to be controlled to transmit and receive at least some data only when in such physical proximity to a second credential communication device as to effectively exclude the possibility of third party involvement in the transmission and reception of said data, wherein said communication means includes at least three separately identifiable ~~**trusted**~~ light indicators**, and**

c. means to communicate the results of processing to effect credential verification.

14. **(PREVIOUSLY PRESENTED)** A credential communication device as in claim 13 wherein said light indicators are formed as bands around the device to facilitate visibility from multiple angles.

15. **(PREVIOUSLY PRESENTED)** A credential communication device as in claim 14 wherein said light indicators are light emitting diodes.

16. **(CURRENTLY AMENDED)** A credential communication device as in claim 1 further including ~~**a trusted alpha-numeric**~~ **an alpha-numeric** display.

17. **(PREVIOUSLY PRESENTED)** A credential communication device as in claim 1 further including a biometric authentication apparatus.

18. **(ORIGINAL)** A credential communication device as in claim 17 wherein said biometric authentication apparatus is a fingerprint scanner.

19-20. **(CANCELED)**

21. **(PREVIOUSLY PRESENTED)** ~~**A credential communication device as in claim 20 wherein**~~ **A credential communication device adapted to transmit and receive data, including:**

a. means to process said data in order to effect mutual credential verification and mutual recognition between the device and a second credential communication device, without reference to a third party,

b. at least one proximity conductor adapted to be controlled to transmit and receive at least some data only when in such physical proximity to a second credential communication device as to effectively exclude the possibility of third party involvement in the transmission and reception of said data,

wherein:

(1) the device is approximately cylindrical, and

(2) the proximity conductor is a bulbous structure **located on the shaft of said approximately cylindrical structure**, permitting momentary contact with a ~~**second device**~~ **second credential communication device** from a variety of angles.

22. **(CURRENTLY AMENDED)** A credential communication device as in claim 1 wherein the device is a component in a mutually authenticated ensemble of devices, the device being adapted to effect data display on a ~~**trusted**~~ remote visual display device.

23. **(ORIGINAL)** A credential communication device as in claim 22 wherein the remote visual display device is a badge display.

24-33. **(CANCELED)**

34. **(CURRENTLY AMENDED)** A method for rapid verification of the credentials of a group of participants by a guard including the steps of:

providing each participant and the guard with a credential communication device as in claim 1,

loading each participant's credential communication devices with data including the identity and credentials of the participant,

operating the guard's device ~~**to cause it**~~ **to cause the device** to seek appropriate identity or credential data from a participant's device,

positioning each participant's device to touch or come into close proximity with the guard's device,

transmitting data and receiving data between the guard's and the participant's devices, the guard's device processing received data to determine the credential status of the participant's device, the guard's device outputting the results of the credential determination.

35. **(ORIGINAL)** The method of claim 34 further including the step of providing a passive device adapted to extend the area in which proximity to the guard's device is sufficient for the proximity conductor to operate.

36. **(CURRENTLY AMENDED)** The method of claim 35 wherein the passive device is a waveguide, adapted to allow the guard's credential communication to be inserted ~~**into it**~~ **into the waveguide**, further including the step of each participant passing ~~**their**~~ **the participant's** credential communication device through the waveguide to communicate ~~**their**~~ **the participant's** credentials.

37. **(CURRENTLY AMENDED)** The method of claim 34 wherein the guard's device is a component in an ensemble including a remote visual display device and further including the step of the guard's credential communication device signalling via secure wireless means to the remote visual display means ~~**in its own ensemble**~~ a visual depiction of the participant associated with the participant's device.

38-41. **(CANCELED)**

42. **(CURRENTLY AMENDED)** A credential communication device as in claim 11 wherein said communication means include ~~**a trusted alpha-numeric**~~ **an alpha-numeric** display.

43. **(CURRENTLY AMENDED)** ~~**A credential communication device as in claim 1**~~ **A credential communication device adapted to transmit and receive data, including:**

a. **means to process said data in order to effect mutual credential verification and mutual recognition between the device and a second credential communication device, without reference to a third party,**

b. **at least one proximity conductor adapted to be controlled to transmit and receive at least some data only when in such physical proximity to a second credential communication device as to effectively exclude the possibility of third party involvement in the transmission and reception of said data,** wherein the proximity conductor is a bulbous structure, permitting momentary contact with a ~~**second device**~~ **second credential communication device** from a variety of angles.

44. **(CURRENTLY AMENDED)** A method for mutual suspicion credential exchange including the steps of:
providing each participant with a credential exchange device as in claim 1,
loading the credential exchange device with credential data relevant to a user,
each participant operating ~~their~~ **the participant's** device to seek appropriate credential data from a second device,
each participant positioning ~~their~~ **the participant's** device to touch or come into close proximity with a second device,
each device transmitting data to and receiving data from a second device,
each device processing received data to determine the credential status of the second device,
each device outputting the results of the credential determination.

45. **(CURRENTLY AMENDED)** The method of claim 44 further including the steps of communicating an ~~organisational~~ **organizational** mandatory security policy to the credential exchange device, and the device applying said mandatory security policy to the data transmitted to the second device.

46. **(CURRENTLY AMENDED)** The method of claim 45 wherein the communication of the ~~organisational~~ **organizational** mandatory security policy is restricted to being a one-off process performed when the device is manufactured or first activated.

47. **(CURRENTLY AMENDED)** The method of claim 45 wherein the mandatory security policy is communicated to the credential communication device by means ~~localised~~ **localized** to the particular location in which the device is operating.

48. **(PREVIOUSLY PRESENTED)** The method of claim 47 wherein said policy communication is by secure wireless means.

49. **(PREVIOUSLY PRESENTED)** The method of claim 44 further including the steps of communicating a user discretionary security policy to the credential exchange device, and the device applying said user discretionary security policy to the data transmitted to the second device.

50. **(CURRENTLY AMENDED)** The method of claim 49 wherein the communication of the user discretionary security policy ~~**is restricted to being a one-off process performed when the device is manufactured or first activated**~~ **occurs only once, and occurs upon manufacture or first activation of the device**.

51. **(CURRENTLY AMENDED)** The method of claim 44 including the step of the credential communication device signalling via secure wireless means to a remote visual display means ~~**in its own ensemble**~~ a visual depiction of the participant associated with the second device.